U.S. DISTRICT COURT FILED APR 13 2017 S.D. OF N.Y.

ORIGINAL

Approved: [signature]
KATHERINE C. REILLY
Assistant United States Attorney

DOC #

Before: THE HONORABLE ANDREW J. PECK
United States Magistrate Judge
Southern District of New York

17 MAG 2798

UNITED STATES OF AMERICA - v. - DMITRY SAZONOV, Defendant.	**COMPLAINT** Violation of 18 U.S.C. §§ 1832 and 2 COUNTY OF OFFENSE: NEW YORK

SOUTHERN DISTRICT OF NEW YORK, ss.:

WILLIAM MCKEEN, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation (the "FBI"), and charges as follows:

COUNT ONE
(Attempted Theft of Trade Secrets)

1. From at least on or about February 3, 2016 through on or about April 12, 2017, in the Southern District of New York and elsewhere, DMITRY SAZONOV, the defendant, with the intent to convert a trade secret that is related to a product and service used in and intended for use in interstate and foreign commerce, to the economic benefit of others than the owner thereof, and intending and knowing that the offense would injure the owner of that trade secret, knowingly did steal, and without authorization appropriate, take, carry away, and conceal, and by fraud, artifice and deception obtain such information; and without authorization did copy, duplicate, sketch, draw, photograph, download, upload, alter, destroy, photocopy, replicate, transmit, deliver, send, mail, communicate, and convey such information; and attempted to do so, to wit, SAZONOV attempted to steal and to convert to his own use the computer source code underlying proprietary trading

software, which was a trade secret of a financial services company for which SAZONOV worked.

(Title 18, United States Code, Sections 1832 and 2.)

The basis for my knowledge and for the foregoing charges are, in part, as follows:

2. I am a Special Agent with the FBI, and I have been personally involved in the investigation of this matter. I have been a Special Agent with the FBI since approximately July 2016. Since becoming a Special Agent with the FBI, I have been assigned to a computer intrusion squad in the FBI's New York Field Office; for approximately two years prior to becoming a Special Agent with the FBI, I served as a Tactical Analyst assigned to that same computer intrusion squad. In those roles, I have participated in numerous investigations of computer crimes. This affidavit is based upon my own observations, conversations with witnesses, and conversations with other law enforcement agents, as well as on my examination of reports and records prepared by others. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all of the facts that I have learned during the course of this investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

3. In the course of this investigation, I have spoken to representatives of a financial services firm engaged in the trading of a variety of publicly traded securities and other financial products ("Firm-1") and reviewed publicly available documents and records. Based on those conversations and that review, I am aware of the following information, in substance and in part, regarding the operations of Firm-1:

a. Firm-1 acts as a market maker, facilitating trading and liquidity in a variety of financial markets. Firm-1, for example, engages in millions of dollars of options trading each day.

b. Firm-1 is headquartered in Pennsylvania and maintains offices in New York, New York, among other locations.

c. A substantial portion of the trading done by Firm-1's employees is facilitated by Firm-1's "automated trading system," a proprietary computer trading platform (the "Trading Platform"), which deploys a computer program to take in many different pieces of market data, to use that data to develop trading strategies, and then to generate orders and automatically submit those orders to an exchange or market center.

d. Traders employed by Firm-1 utilize the Trading Platform in executing trades involving publicly traded securities and other financial products in interstate commerce. Firm-1's use of the Trading Platform accounts for a substantial volume of Firm-1's total trading activity. For example, Firm-1 executes approximately $300 million in options trades through the Trading Platform every day.

e. The strategies and efficiency resulting from Firm-1's use of the Trading Platform contribute substantially to Firm-1's market share in the financial markets in which Firm-1 trades and to its overall trading profits.

f. For at least approximately five years, Firm-1 has been in the process of developing an updated and improved version of the Trading Platform (the "Updated Trading Platform"). Firm-1 has, to date, invested over $5 million in the development of the Updated Trading Platform. The Updated Trading Platform is expected by representatives of Firm-1 to continue to enhance the position of Firm-1 in the markets in which it participates. While the Updated Trading Platform is still in development, Firm-1 has deployed the Updated Trading Platform as a pilot program; the Updated Trading Platform has been used, for example, to execute options trades.

g. The Trading Platform and the Updated Trading Platform are proprietary to Firm-1 and contribute substantially to Firm-1's market share and profits. The economic value of the Trading Platform and the Updated Trading Platform depend, at least in part, on their remaining undisclosed and proprietary.

h. Public disclosure of the computer source code that comprises the Updated Trading Platform (the "Source Code") would undermine the competitive advantage achieved by Firm-1 as a result of use of the Trading Platform and the

Updated Trading Platform. Even disclosure of the Source Code to a competitor of Firm-1 could also erode Firm-1's market share in the markets in which it trades and erode its relative advantage. Because of the proprietary nature of the Updated Trading Platform, Firm-1 has put in place a variety of measures designed in part to protect the Source Code from disclosure to a competitor or to the public. For example:

i. Firm-1 does not permit its employees to utilize external e-mail or file sharing websites. Firm-1 further does not permit its employees to download data from their work computers to USB drives or other portable storage devices.

ii. Firm-1 employees use a unique login identifier and password to log into a software repository platform (the "Software Repository"). Even within the Software Repository, only Firm-1 employees involved in the development of the Updated Trading Platform are permitted to access the Source Code.

iii. Employees of Firm-1 sign agreements detailing the confidential nature of Firm-1's work and Firm-1's ownership of work product developed in the course of that work. Employees involved in the technological aspects of Firm-1's work also sign additional agreements that govern work they may do for competitors in the period following any termination of employment.

4. In the course of this investigation, I have spoken to employees and representatives of Firm-1, including, among others, technical analysts retained by Firm-1. I have also reviewed documents and records, including documents and records provided by an e-mail provider (the "Provider") in response to subpoenas and to a judicially authorized search warrant. Based on those conversations and that review, I am aware of the following information, in substance and in part, regarding the employment of DMITRY SAZONOV, the defendant, by Firm-1:

a. Beginning in or about July 2004 through on or about February 6, 2017, DMITRY SAZONOV was employed as a software engineer by Firm-1. Most recently and as of the date of his termination on or about February 6, 2017, SAZONOV worked in the New York, New York office of Firm-1.

b. In his capacity as a software engineer for Firm-1, SAZONOV was supervised by and directly supported an individual employed by Firm-1, who was involved in developing trading strategies for Firm-1 ("Individual-1"). SAZONOV and Individual 1 were both directly involved in the development of trading strategies to be implemented in conjunction with the deployment of the Updated Trading Platform. As a result, SAZONOV had access to the Source Code in the Software Repository.

c. SAZONOV was also supervised by another individual ("Individual-2") involved in the technological work of Firm-1, who was based in Firm 1's Pennsylvania headquarters.

d. On or about February 2, 2017, SAZONOV and others employed by Firm-1 were informed by an employee of Firm-1 that Individual-1 had resigned from Firm-1.

e. Representatives of Firm-1 have reviewed records of SAZONOV's Internet and computer activity using his Firm-1 desktop computer and have voluntarily disclosed the results of that review to law enforcement agents. Those records demonstrate that on or about February 2, 2017, SAZONOV conducted searches of the Internet for software developer positions in New York, New York and reviewed his résumé.

f. On or about Friday, February 3, 2017, Individual-2 contacted SAZONOV to inform him, in substance and in part and among other things, that Individual-2 would meet with SAZONOV in Firm-1's New York, New York office on Monday, February 6, 2017 at approximately 3 p.m. to discuss SAZONOV's future with Firm-1 in light of Individual-1's departure.

g. Based upon documents and records produced by the Provider, I am aware that SAZONOV is the subscriber associated with an e-mail account maintained by the Provider ("E-mail Account-1"). Based on my review of documents and records produced by the Provider in response to a judicially authorized search warrant, I am aware that between on or about February 2, 2017 and on or about February 5, 2017, SAZONOV used E-mail Account-1 to contact several recruiters and headhunters seeking employment opportunities for software developers. For example, in an e-mail sent to a recruiter on or about February

3, 2017, SAZONOV wrote, in substance and in part, that he had been "working for [Firm-1] for over 13 years, developed core trading systems for them[.] Wonder if you have openings in other Wall Street companies and what is salaries this [*sic*] days."

5. In the course of this investigation, I have spoken to employees and representatives of Firm-1, including, among others, technical analysts retained by Firm-1. I have also reviewed documents and records, including documents and records produced by the Provider. Based on those conversations and that review, I am aware of the following, in substance and in part, regarding the activities of DMITRY SAZONOV, the defendant, on or about February 6, 2017:

a. On the morning of Monday, February 6, 2017, SAZONOV reported to work at the New York, New York office of Firm-1.

b. At approximately 8:43 a.m., SAZONOV logged on to the Firm-1 computer system.

c. At approximately 8:57 a.m., SAZONOV logged into the Software Repository. SAZONOV subsequently downloaded the Source Code.

d. At approximately 9:45 a.m., SAZONOV created a zip file containing the Source Code ("Zip File-1").

e. Also at approximately 9:45 a.m., SAZONOV created a PDF file (the "PDF File"). Later in the day, at approximately 1:53 p.m., SAZONOV placed the PDF file into an encrypted Zip File ("Zip File-2"). Though the PDF file cannot be opened at present because Zip File-2 is encrypted, the PDF file is of exactly the same size as, and was created at the same time as, the file contained in Zip File-1; the PDF file also bears the same name as the file contained in Zip File-1, but with a ".PDF" extension. As a result, and based on my training and experience in financial computer crime and computer forensics, I believe that the PDF file contains the same data as the file contained in Zip File-1, specifically that it is a file containing the Source Code.

f. During the course of the day on or about February 6, 2017, SAZONOV used his Firm-1 computer to run

Internet searches related to steganography, the practice of concealing messages or data within other files, among other things. SAZONOV also reviewed posts on a website described as an online community for programmers ("Website-1") that related to steganography. For example, at or about 10:59 a.m. on or about February 6, 2017, SAZONOV used his Firm-1 computer to visit a page of Website-1 that discussed how to "append data" to an existing file.

g. On or about February 6, 2017, after creating Zip File-1 and Zip File-2, SAZONOV created and ran an executable file (the "Executable File"), which appears to have deployed steganography, in order to break up the PDF file believed to contain the Source Code, and append pieces of the PDF file to various apparently innocuous documents and files contained in a folder on SAZONOV's desktop computer, including personal tax and immigration documents and images taken from the Internet, among others (the "Payload Documents"). The resulting Payload Documents appear to be completely innocuous; based on the analysis conducted of the Executable File, and on my training and experience, I believe that they do, however, contain the Source Code. The Executable File also produced a manifest (the "Manifest File") that lists each of the files with this appended data and the amount of data appended. Based on my training and experience in financial computer crime and computer forensics, I believe that SAZONOV or another individual could have utilized the Executable File, the Manifest, and the Payload Documents in combination to reconstruct the Source Code.

h. SAZONOV then took steps that appear to have been designed to remove the Executable File, the Manifest File, and the Payload Documents from Firm-1's New York, New York office.

i. Between approximately 2:44 p.m. and 2:45 p.m., SAZONOV saved two draft e-mails in his Firm-1 e-mail account. These draft e-mails were both addressed to an e-mail account administered by the Provider ("E-mail Account-2"). One of the draft e-mails attached an encrypted zip file ("Zip File-3") containing the Manifest File. The other draft e-mail attached an unencrypted zip file ("Zip File-4") containing the Payload Documents. Though SAZONOV prepared these two e-mails to be sent, he did not send them before his meeting with Individual-2.

i. Based upon documents produced by the Provider, I am aware that the subscriber of E-mail Account-2 appeared to use a fictitious name ("Name-1") in setting up E-mail Account-2. However, based upon my training and experience and my review of documents and records produced by the Provider, as set forth below, I believe that SAZONOV is the user of E-mail Account-2.

(1) The recovery e-mail address for E-mail Account-2 is E-mail Account-1, for which SAZONOV is the subscriber. Additionally, the recovery e-mail address for E-mail Account-1 is E-mail Account-2.

(2) Between in or about January 2017 and in or about February 2017, an individual using Name-1 and E-mail Account-2 made purchases through an online retailer that were shipped and billed to SAZONOV at a residential address ("Address-1"). Additionally, on or about February 21, 2017, an invoice was sent to E-mail Account-2 by an auto body shop, which listed the customer as SAZONOV at Address-1. SAZONOV had previously identified Address-1 as his home address in forms completed in connection with his employment by Firm-1.

(3) In or about February and March 2017, SAZONOV appears to have used E-mail Account-2 to correspond with headhunters and recruiters regarding computer software positions, including in e-mails that copy E-mail Account-1.

j. At approximately 2:47 p.m., SAZONOV logged into an external website, which was unaffiliated with Firm-1, and uploaded Zip File-3.

k. At approximately 2:50 p.m., SAZONOV printed a copy of the code comprising the Executable File. Representatives of Firm-1 subsequently searched SAZONOV's office but did not find this print out.

l. At approximately 3:00 p.m., SAZONOV met with Individual-2 in Firm-1's New York, New York office. A Human Resources employee of Firm-1 ("Individual-3") joined the meeting by telephone. In the course of the meeting, SAZONOV was fired by Firm-1. SAZONOV repeatedly asked, in substance and in part, to return to his desk to retrieve files from his computer.

Pursuant to Firm-1 policy, SAZONOV was not permitted to return to his desk prior to being escorted out of Firm-1's New York, New York office.

6. In the course of this investigation, I have spoken to employees of Firm-1. I have also reviewed documents and records, including documents and records provided voluntarily by Firm-1 and provided by the Provider in response to subpoenas and to a judicially authorized search warrant. I have further reviewed a consensual recording of a telephone conversation between Individual-3, acting at the direction of law enforcement, and DMITRY SAZONOV, the defendant. Based on those conversations and that review, I am aware of the following, in substance and in part, regarding the activities of SAZONOV following his termination from Firm-1:

a. On multiple occasions following his termination by Firm-1, SAZONOV contacted individuals employed by Firm-1 by telephone and by e-mail seeking the return of computer files on his Firm-1 desktop computer, which he claimed were personal documents.

b. On or about February 6, 2017, at approximately 3:36 p.m., SAZONOV e-mailed Individual-3. In that e-mail communication, SAZONOV requested, in substance and in part, that Individual-3 send everything in a specific folder ("Folder-1") on his Firm-1 computer's hard drive to him, including, specifically, Zip File-4 (containing the Payload Documents), which was saved within Folder-1. SAZONOV wrote, in substance and in part, that Folder-1 and Zip File-4 contained "important tax and INS information." SAZONOV also requested, in substance and in part, that various other personal documents be returned to him.

c. On or about February 7, 2017, SAZONOV again e-mailed Individual-3, asking, in substance and in part, "what is the status of my personal files" and asking that something be done before Firm-1 took steps to "wipe out hard drive."

d. On or about March 22, 2017, Individual-3 and SAZONOV spoke by telephone. In the course of that telephone call, SAZONOV requested that the files contained in Folder-1, and other personal files on his Firm-1 computer, be returned to him. SAZONOV stated, in substance and in part, that he moved personal files into Folder-1 before being terminated because he "was afraid [he] might be laid off" and wanted to separate personal files from any work product. In response to a question from Individual-3, SAZONOV further confirmed that the files in Folder-1 were all personal files and didn't contain "any [Firm-1]-related stuff."

e. On or about April 7, 2017, Individual-3, acting at the direction of law enforcement, e-mailed SAZONOV, writing, in substance and in part, that he could pick up a disk containing his "requested files" on or about Wednesday, April 12, 2017 in the lobby of the office building in which the New York, New York office of Firm-1 is located. SAZONOV responded to Individual-3 by e-mail later on or about April 7, 2017, writing, in substance and in part, that he was "confirm[ing] meeting" with a representative of Firm-1 on "Wednesday 10:00[.]"

7. Based on my involvement in this investigation and my conversations with other law enforcement agents, I am aware of the following, in substance and in part:

a. On or about the morning of April 12, 2017, a law enforcement agent ("Agent-1") posing as an employee of Firm-1 placed a telephone call to DMITRY SAZONOV, the defendant. SAZONOV informed Agent-1, in substance and in part, that he could not come to Firm-1's New York, New York office that morning as planned because he had a job interview. SAZONOV proposed, in substance and in part, that he instead come to Firm-1's New York, New York office later that day. Agent-1 and SAZONOV had multiple additional telephone calls on or about April 12, 2017 to confirm the meeting.

b. On or about the late afternoon of April 12, 2017, SAZONOV arrived in the lobby of the office building in which the New York, New York office of Firm-1 is located. Agent-1, posing as an employee of Firm-1, approached SAZONOV and gave him the disk purportedly containing the electronic files he had sought from Firm-1. SAZONOV accepted the disk from Agent-1. SAZONOV then requested, in substance and in part, that additional personal items be returned to him.

c. SAZONOV was then approached by law enforcement agents and placed under arrest.

WHEREFORE, I respectfully request that DMITRY SAZONOV, the defendant, be imprisoned or bailed, as the case may be.

WILLIAM MCKEEN
Special Agent
Federal Bureau of Investigation

Sworn to before me this
13th day of April, 2017

THE HONORABLE ANDREW J. PECK
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK